UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,139	05/22/2001	Roy F. Quick JR.	010055B1	1058

23696 7590 08/24/2005

Qualcomm Incorporated
Patents Department
5775 Morehouse Drive
San Diego, CA 92121-1714

EXAMINER	
MOORTHY, ARAVIND K	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 08/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/863,139	QUICK ET AL.	
	Examiner	Art Unit	
	Aravind K. Moorthy	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *20 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed on 7 June 2005.

2. Claims 1-17 are pending in the application.

3. Claims 1-17 have been rejected.

Response to Arguments

4. Applicant's arguments filed 7 June 2005 have been fully considered but they are not persuasive.

On page 9, the applicant argues that there is nothing in DeTreville to even suggest generating an initial value based upon a first key from the plurality of keys generated in response to a received challenge.

The examiner respectfully disagrees. DeTreville teaches generating a plurality of keys in response to a received challenge from the portable IC device. DeTreville teaches generating a initial value, by using a seed generator, based upon a first key from the plurality of keys.

On page 9, the applicant argues that DeTreville does not teach or even mention concatenating the initial value with a received signal that is generated using a second key from the plurality of keys generated in response to the challenge.

The examiner respectfully disagrees. DeTreville teaches concatenating the seed value with the SIR value that is generated using a second key from the plurality of keys generated in response to the challenge.

On page 10, the applicant argues that Zhang does not suggest a concatenation of a secret key with information from a mobile unit.

The examiner respectfully disagrees. Zhang teaches concatenating verification information from the mobile unit with a secret key.

On page 10, the applicant argues that Zhang does not teach or even mention generating a signature by concatenating a secret key with information from a mobile unit as in claim 8.

The examiner respectfully disagrees. Zhang teaches generating signature from the concatenation of the verification information from the mobile unit and a secret key.

On page 10, the applicant argues that Zhang does not teach or even suggest generating a plurality of keys from a received value and a secret value as in claim 11.

The examiner respectfully disagrees. Zhang teaches generating a plurality of keys from device identifiers and the received initial values.

On page 10, the applicant argues that Zhang does not teach generating an authorization signal from hashing a version of at least one secret key together with an authorization message.

The examiner respectfully disagrees. Zhang teaches generating an authorization signal from hashing the concatenation of the secret key and an authorization message.

On page 11, the applicant argues that Zhang does not teach or suggest generating a signature by hashing a concatenated value formed from a key and a transmission message.

The examiner respectfully disagrees. Zhang teaches verifying the hashed authorization signal by creating a signature over the secret key and the authorization message.

On page 11, the applicant argues that Zhang does not teach or even mention generating a primary signature.

The examiner respectfully disagrees. Zhang teaches verifying the hashed authorization signal by creating a signature over the secret key and the authorization message.

On page 11, the applicant argues that Zhang does not teach or even suggest an apparatus coupled to a mobile station, wherein the apparatus comprises a processor configured to generate a primary signature based on a key that is held private from the mobile station and a secondary signature that is received from the mobile station as in claim 17.

The examiner respectfully disagrees. The primary signature is based upon the secret key. The secondary key is received from the mobile station.

On page 12, the applicant argues that DeTreville does not disclose every element of claims 3, 4, 6 and 7 based on its dependency from claim 1 as well as other novel features included therein. The applicant argues that Deindl does not teach the generation of a plurality of keys, the generation of an initial value and the concatenation as in independent claim 1.

The examiner respectfully disagrees. Deindl was not used to teach the generation of an initial value and the concatenation as in independent claim 1. Deindl was used to teach the deficiencies of claims 3, 4, 6 and 7.

On page 12, the applicant argues that Zhang does not disclose every element of claims 14 and 16 based on its dependency from claims 11 and 15 as well as other novel features included therein. The applicant argues that Deindl does not teach the generation of a plurality of keys, the generation of an initial value and the concatenation as in independent claims 11 and 15.

The examiner respectfully disagrees. Deindl was not used to teach the generation of a plurality of keys, the generation of an initial value and the concatenation as in independent claim 1. Deindl was used to teach the deficiencies of claims 14 and 16.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2 and 5 are rejected under 35 U.S.C. 102(e) as being anticipated by DeTreville U.S. Patent No. 6,609,199 B1.

As to claim 1, DeTreville discloses a memory and a processor configured to implement a set of instructions stored in the memory [column 4, line 7-17]. DeTreville discloses generating a plurality of keys in response to a received challenge [column 5, lines 54-65]. DeTreville discloses generating an initial value based upon a first key from the plurality of keys [column 9, lines 14-21]. DeTreville discloses concatenating the initial value with a received signal to form an input value [column 9, lines 14-21]. DeTreville discloses that the received signal is transmitted from a communications unit communicatively coupled to the subscriber identification module [column 9, lines 22-28]. DeTreville discloses that the received signal is generated by the communications unit using a second key from the plurality of keys, the second key having been communicated from the subscriber identification module to the communications unit [column 9, lines 51-59]. DeTreville discloses hashing the input value to form an authentication signal [column 9, lines 51-65]. DeTreville discloses transmitting the authentication signal to the communications system via the communications unit [column 7, lines 15-35].

As to claim 2, DeTreville discloses that hashing the input value is performed in accordance with the Secure Hashing Algorithm (SHA-1) [column 9, line 60].

As to claim 5, DeTreville discloses receiving the second key from the subscriber identification module [column 9, lines 22-28]. DeTreville discloses generating a local initial value based upon the second key [column 23, lines 24-34]. DeTreville discloses concatenating the local initial value and a message to form a local input value [column 24, lines 1-9]. DeTreville discloses hashing the local input value to form the received signal [column 24, lines 10-25]. DeTreville discloses transmitting the received signal to the subscriber identification module [column 24, lines 38-46].

6. Claims 8-13, 15 and 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Zhang et al U.S. Patent No. 6,516,414 B1.

As to claim 8, Zhang et al discloses a key generation element [column 2, lines 17-40]. Zhang et al discloses a signature generator configured to receive a secret key from the key generation element and information from a mobile unit [column 4, lines 35-63]. Zhang et al discloses generating a signature that will be sent to the mobile unit [column 4, lines 18-34]. Zhang et al discloses that the signature is generated by concatenating the secret key with the information from the mobile unit and hashing the concatenated secret key and information [column 8, lines 32-62].

As to claim 9, Zhang et al discloses that the generation element comprises a memory and a processor configured to execute a set of instructions stored in the memory [column 2, lines 47-63]. Zhang et al discloses that the set of instructions performs a cryptographic transformation

upon an input value to produce a plurality of temporary keys [column 2 line 64 to column 3 line 11].

As to claim 10, Zhang et al discloses that the cryptographic transformation is performed using a permanent key [column 4, lines 35-63].

As to claim 11, Zhang et al discloses a key generator for generating a plurality of keys from a received value and a secret value [column 4, lines 35-63]. Zhang et al discloses that at least one communication key from the plurality of keys is delivered to the communications unit and at least one secret key from the plurality of keys is not delivered to the communications unit [column 4, lines 35-63]. Zhang et al discloses a signature generator for generating an authorization signal from hashing a version of the at least one secret key together with an authorization message [column 11 line 48 to column 12 line 3]. Zhang et al discloses that the authorization message is generated by the communications unit using a version of the at least one communication key [column 11 line 48 to column 12 line 3].

As to claim 12, Zhang et al discloses that the subscriber identification module is configured to be inserted into the communications unit [column 2, lines 47-63].

As to claim 13, Zhang et al discloses that at least one communication key comprises an integrity key [column 13, lines 35-52].

As to claim 15, Zhang et al discloses generating a plurality of keys, as discussed above for claim 8. Zhang et al discloses transmitting at least one key from the plurality of keys to a communications device communicatively coupled to the subscriber identification device and holding private at least one key from the plurality of keys [column 14, lines 29-44]. Zhang et al discloses generating a signature at the communications device using both the at least one key

transmitted to the communications device and a transmission message, as discussed above. Zhang et al discloses that generating is implemented by hashing a concatenated value formed from the at least one key and the transmission message, as discussed above for claim 8. Zhang et al discloses transmitting the signature to the subscriber identification device [column 8, lines 32-62]. Zhang et al discloses receiving the signature at the subscriber identification device [column 8, lines 32-62]. Zhang et al discloses generating a primary signature from the received signature [column 8, lines 32-62]. Zhang et al discloses that the generating is implemented by hashing a concatenated value formed from the at least one private key and the signature received from the communications device [column 11 line 48 to column 12 line 3]. Zhang et al discloses conveying the primary signature to a communications system [column 11 line 48 to column 12 line 3].

As to claim 17, Zhang et al discloses a memory and a processor configured to implement a set of instructions stored in the memory, as discussed above for claim 8. Zhang et al discloses that the set of instructions for selectively generates a primary signature based upon a key that is held private from the mobile station and a secondary signature that is received from the mobile station [column 4, lines 35-63].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 3, 4, 6 and 7 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeTreville U.S. Patent No. 6,609,199 B1 as applied to claim 1 above, and further in view of Deindl et al U.S. Patent No. 6,076,162.

As to claims 3, 4, 6 and 7, DeTreville does not teach that generating the initial value comprises padding the first key. DeTreville does not teach that generating the initial value further comprises adding the padded first key bit-wise to a constant value. DeTreville does not teach that generating the local initial value comprises padding the second key. DeTreville does not teach that generating the local initial value further comprises adding the padded second key bit-wise to a second constant value.

Deindl et al teaches padding a key and adding the padded key bit-wise to a constant value.

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified DeTreville so that the initial values would have been generated by padding the first and second key and adding both of the padded keys to a constant value.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified DeTreville, as described above, by the teaching of Deindl et al because data can be extended to fill up any necessary block length [column 4, lines 46-56].

8. Claims 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Zhang U.S. Patent No. 6,516,414 B1 as applied to claims 11 and 15 above, and further in view of Applied Cryptography (hereinafter Schneier).

As to claims 14 and 16, Zhang discloses using hash functions, as discussed above.

Zhang does not teach that the hash function is the Secure Hash Algorithm (SHA-1).

Schneier teaches the Secure Hash Algorithm (SHA-1) and its benefits [pages 442-445].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zhang so that the hashing function was the Secure Hash Algorithm (SHA-1).

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Zhang by the teaching of Schneier, as described above, because there are no known cryptographic attacks against SHA and it is more resistant to brute-force attacks [page 445].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Primary Examiner
AU 2131
8/20/05

Aravind K Moorthy AM
August 19, 2005